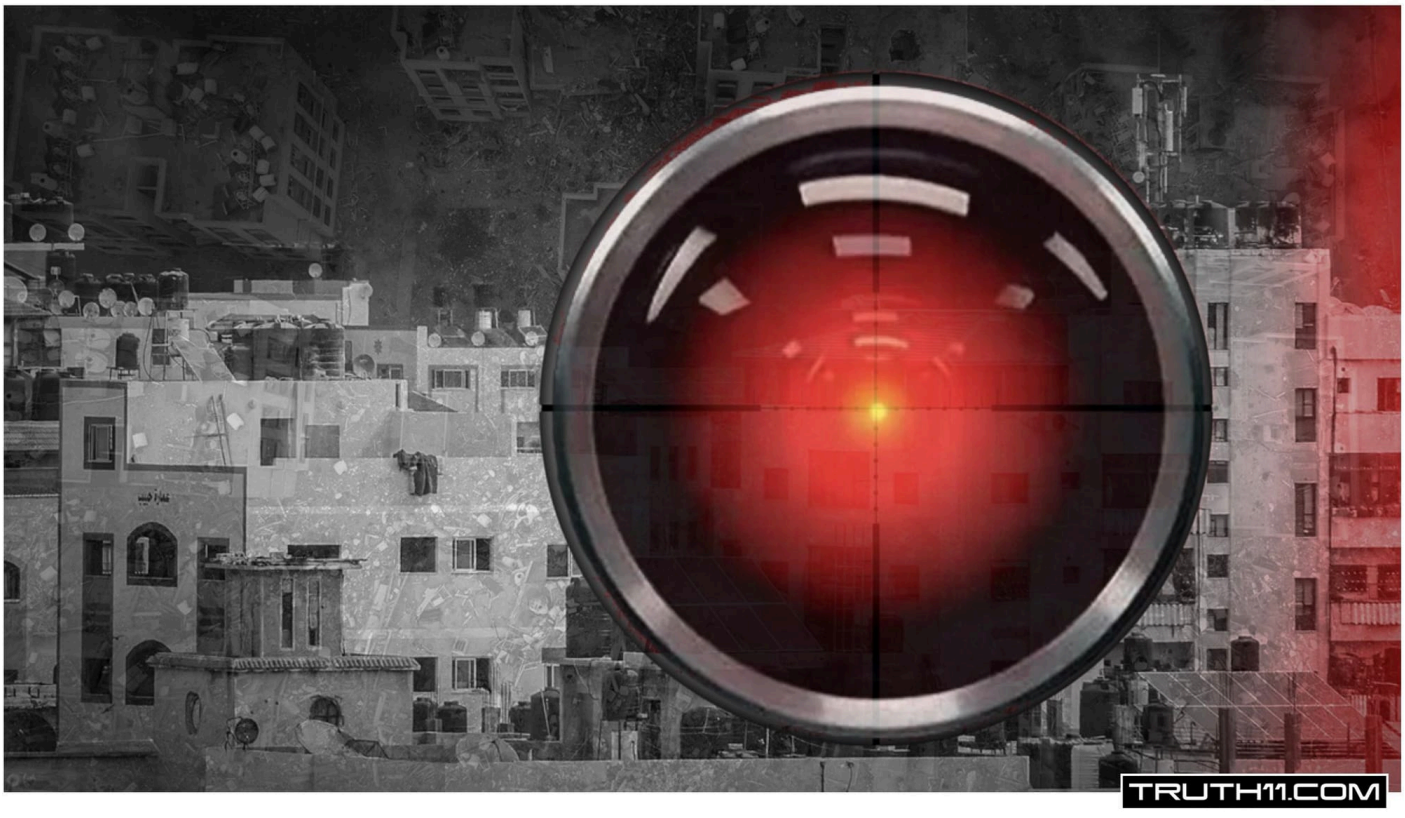
AI-Powered Genocide | Twenty Seconds to Mark a Human for Death

TRUTH11.COM

Oct 29, 2025 15 min



Silicon Valley's AI Infrastructure Behind Gaza Genocide

TheLibertyBeacon.com

The promotional videos show smiling engineers. The press releases promise "AI for Good." But in Gaza, the sanitized language of tech innovation collides with a brutal

reality in which artificial intelligence systems designed in Silicon Valley are now choosing who lives and who dies. Marwa Fatafta, a Palestinian researcher and policy analyst based in Berlin, has spent months documenting how this happened. Her new report reveals something that should shake us all. Big Tech's cloud computing and AI tools aren't just being used in Israel's war on Gaza; they've become essential infrastructure for what multiple UN bodies have called genocidal acts.

Twenty Seconds to Mark a Human for Death

Inside Israeli military operations centers, AI systems with names like "Lavender," "The Gospel," and "Where's Daddy?" are running around the clock. They're not assisting human decisions so much as replacing them.

Lavender can identify and approve a target in just 20 seconds. Think about that. In the time it takes to read this paragraph, the system has already decided someone should die.

The scale is breathtaking in its horror. According to reports from Israeli military sources, Lavender generated a list of 37,000 people it identified as Hamas members. Many were low-ranking. Some had no confirmed military roles at all. The Israeli military was striking as many as 250 targets daily, more than double the rate of previous conflicts. By December 2023, more than 22,000 targets had been hit inside Gaza, a pace that would be impossible without algorithmic automation.

Then there's "Where's Daddy?", a system that reportedly tracks militants through their mobile phones and waits. It waits until they go home. Until they're with their families. The system treats their presence at home as confirmation of identity. And then it strikes.

One senior Israeli military source described how it works: each target comes with a "collateral damage score", a calculation of how many civilians will likely die. Operators, the source said, use "very accurate" measurements of how many civilians evacuate a building just before a strike. Another military insider compared it to "a traffic signal."

Families become acceptable losses. Homes become kill boxes. Children become collateral, their deaths pre-calculated and deemed acceptable.

The Cloud Services Behind the Killing

Here's where American companies enter the story.

Between October 7, 2023, and the following March, the Israeli military's use of Microsoft and OpenAI artificial intelligence spiked to nearly 200 times pre-war levels. The data it stored on Microsoft servers doubled by July 2024, reaching more than 13.6 petabytes, roughly 350 times the digital memory needed to store every book in the Library of Congress.

The AI models powering these systems? They come from OpenAI, the maker of ChatGPT, delivered through Microsoft's Azure cloud platform and purchased by the Israeli military.

> *"This is the first confirmation we have gotten that commercial AI models are directly being used in warfare," says Heidy Khlaaf, chief artificial intelligence scientist at the AI Now Institute.*

At a 2014 military conference, titled "IT for IDF", the implications became starkly visual, as Col. Racheli Dembinsky, a senior Israeli military IT officer, described how AI had provided "very significant operational effectiveness" in Gaza, the logos of Microsoft Azure, Google Cloud, and Amazon Web Services appeared on the screen behind her. "We've already reached a point where our systems really need it," she said.

Google and Amazon aren't bystanders either. Through Project Nimbus, a $1.2 billion contract signed in 2021, both companies provide cloud computing and AI services directly to the Israeli Defense Forces. And there are suggestions that even Meta is implicated: metadata from WhatsApp may be feeding the Lavender targeting system.

Gaza as Laboratory

This isn't new territory for Gaza. For decades, Israel has used the Strip as what amounts to a live testing ground for weapons and surveillance technologies. What gets tested in Gaza gets refined, packaged, and sold globally.

The surveillance feeding these AI systems is equally chilling. A New York Times investigation revealed that the Israeli military deployed an expansive facial recognition system across Gaza, "collecting and cataloging the faces of Palestinians without their knowledge or consent." Social media activity, phone records, daily routines, all of it captured, analyzed, and fed into AI systems that turn ordinary life into targeting data.

Your morning commute, your phone calls, where you pray and where your children go to school; All of it becomes intelligence, and all of it makes you targetable.

The Legal Reckoning

In September 2025, the UN Independent International Commission of Inquiry on the Occupied Palestinian Territory concluded that Israel has committed genocide against Palestinians in Gaza. The Commission found that Israeli authorities committed four of the five genocidal acts defined by the 1948 Genocide Convention.

A legal opinion commissioned by human rights organizations Al-Haq and SOMO suggests tech companies providing services essential to Israeli military operations may be directly contributing to violations of international humanitarian law, and possibly to genocidal acts. The analysis notes that under international criminal law, "direct complicity requires intentional participation, but not necessarily an intention to do harm, only knowledge of foreseeable harmful effects."

In other words, ignorance is not a defense.

UN Special Rapporteur Francesca Albanese has named 48 corporate actors, including Microsoft and Google's parent company Alphabet, as aiding Israel's war on Gaza in breach of international law. Her report found "reasonable grounds" to believe Palantir provided technology used for automated battlefield decision-making and target list generation through AI systems like Lavender.

Ben Saul, another UN special rapporteur, put it bluntly: if the reports about Israel's AI use are accurate, "many Israeli strikes in Gaza would constitute the war crimes of launching disproportionate attacks."

The Human Toll

The numbers are staggering, but they don't capture the reality. Since the war began, more than 60,000 people have died in Gaza, notwithstanding those who lost their lives in Lebanon. Some reports are suggesting another hundred thousand dead beneath the rubble in the Strip, whilst data shows nearly 70% of Gaza's buildings have been destroyed or damaged.

> *Behind every statistic is a name. A face. A life.*
>
> *"When a 3-year-old girl is killed in a home in Gaza, it's because someone in the army decided it wasn't a big deal for her to be killed, that it was a price worth paying in order to hit [another] target," one Israeli military intelligence source told +972Magazine. "These are not random rockets. Everything is intentional. We know exactly how much collateral damage there is in every home."*

The systems themselves are fundamentally flawed. A report by the Jewish Institute for National Security of America (JNSA) identified a critical problem: the system had data on what constituted a target, but no data on what didn't. Intelligence that human analysts had examined and deemed non-threatening had simply been discarded. The AI learned only from positive examples of targets, creating inevitable bias.

> *"The fact that AI systems are being used indicates there's a lack of regard by the Israeli state," says UCLA professor Ramesh Srinivasan. "Everybody knows these AI systems will make mistakes."*

And yet, according to reports, many operators trusted Lavender so completely that they approved its targets without checking them at all.

Dissent from Within

Not everyone inside these companies is comfortable.

Employees at Amazon, Google, Microsoft, and Palantir have publicly questioned their employers' roles in AI-driven warfare. Some have cited possible complicity in war crimes. Microsoft faced internal backlash for providing Azure services to Unit 8200, Israel's signals intelligence unit. After The Guardian reported that data from mass surveillance in Gaza and the West Bank, including phone call records, was being used to identify bombing targets, Microsoft opened an inquiry. In September 2024, the company ended Unit 8200's access to Azure services.

But as Paul Scharre of the Center for a New American Security (CNAS) warns, "The pace of technology is far outstripping the pace of policy development."

The damage has been done. The precedent has been set.

The Collapse of "AI for Good"

Under slogans like "AI for Good," tech companies have promised us ethical innovation and social progress. They've spoken of democratizing information, connecting humanity, and solving global challenges. However, in Gaza, those promises lie in ruins, literally, amid the rubble of algorithmically-targeted homes.

What we're witnessing is the apotheosis of AI's most dangerous trends: biometric mass surveillance, predictive policing, and automated decision-making over life and death. Technologies that human rights advocates have argued should be banned even in peacetime are now being deployed in what UN experts are unequivocally calling a genocide.

> *"When clear signs and evidence of genocide emerge, the absence of action to stop it amounts to complicity," said Commission Chair Navi Pillay. "Every day of inaction costs lives and erodes the credibility of the international community."*

What Comes Next

Gaza has answered one question definitively: AI can be and is being weaponised for mass killing.

But two questions remain. Will we allow the corporations profiting from this violence to escape accountability? Will Silicon Valley's giants face consequences for providing the infrastructure of genocide, or will they continue collecting their billion-dollar contracts while issuing hollow statements about ethical AI?

And will the international community permit this new paradigm of automated, algorithmic killing to become normalized? Will "Where's Daddy?" and systems like it become the template for tomorrow's wars?

In Gaza right now, a child is playing. An algorithm may already be watching. A server farm in California may already be calculating his/her death. A corporation may already be profiting.

The future of warfare isn't coming. It's here. And it's being built by companies whose logos we see every day, whose products we carry in our pockets, whose services we use without thinking.

The only question left is: what are we going to do about it?

Freddie Ponton, 21st Century Wire

Marwa Fatafta | Al-Shabaab.org

AI for War: Big Tech Empowering Israel's Crimes and Occupation

Executive Summary

US technology giants present themselves as ethical innovators shaping a better world through artificial intelligence (AI) and cloud computing. Yet in Gaza, these narratives have collapsed. AI systems, cloud infrastructures, and surveillance tools supplied by tech companies such as Google, Amazon, Microsoft, and Palantir have become integral to Israel's genocidal campaign against Palestinians.

Introduction

US technology giants portray themselves as architects of a better world powered by artificial intelligence (AI), cloud computing, and data-driven solutions. Under slogans such as "AI for Good," they pledge to serve as ethical stewards of the technologies reshaping our societies. Yet in Gaza, these narratives have collapsed, alongside international norms and what remains of the so-called rules-based order.

The Israeli regime's genocidal war in Gaza has drawn attention to the role of major technology companies in enabling military operations and sustaining the occupation. Beneath the Israeli destruction lie servers, neural networks, and software systems built and deployed by some of the world's most powerful corporations. The increasing militarization of digital technologies and infrastructures, most visibly in Israel's deployment of AI-driven systems and data analytics in Gaza, has reshaped debates on accountability and exposed critical gaps in existing governance frameworks. This policy brief examines how the frontier of accountability for technology companies now extends to potential complicity in war crimes, crimes against humanity, and genocide, underscoring the urgent need for new approaches to regulating AI militarization.

An AI-Powered Genocide

The Israeli regime first deployed AI systems to generate and prioritize lethal targets during the 11-day bombardment of Gaza in May 2021, a vicious, unlawful assault the Israeli military later described as its first "AI war." Since then, the occupation forces have significantly expanded their reliance on AI tools, using cloud computing and machine learning to store and process vast volumes of surveillance data, from satellite imagery to intercepted communications, to automate the identification and ranking of targets for attack.

Central to Israel's AI warfare is Project Nimbus—a $1.2 billion contract through which Google and Amazon have provided the Israeli government and military with advanced cloud infrastructure and machine learning capabilities. In the early days of the genocide, Israeli forces reportedly relied almost entirely on AI-powered target-generating systems—such as Lavender, The Gospel, and Where's Daddy—to accelerate mass killing and destruction across Gaza. These platforms ingest mass

surveillance data about the entire population of Gaza to algorithmically determine—at scale—who is to be killed, which buildings are to be bombed, and how much "collateral damage" is deemed acceptable.

Alarmingly, these AI-driven systems internalize the genocidal logic of their operators. They are trained to treat civilians as "terrorists," building on the genocidal logic of Israeli officials who declared that "there are no innocent civilians in Gaza." As part of efforts to automate lethal targeting, military commanders reportedly instructed soldiers to identify and feed as many targets as possible into the system. This effectively lowers the threshold for designating individuals as "Hamas militants," casting a wide net of algorithmically flagged subjects. Despite its high error rate, the only criterion Israeli soldiers applied to Lavender's kill list was the target's gender, effectively rendering all Palestinian males—children and adults alike—legitimate targets. In practice, AI technology has enabled the Israeli regime's genocidal logic to be executed with ruthless, machine-driven efficiency, reducing Palestinians, their families, and their homes to what the military chillingly refers to as "garbage targets."

While many of the technical details of Israel's AI targeting systems remain classified, there is ample credible evidence that their functionality depends on cloud infrastructure and machine-learning capabilities developed and maintained by major technology companies, including Google, Amazon, Microsoft, and Palantir. Consequently, tech companies' direct provision of digital systems used in Israeli warfare raises urgent questions about corporate complicity in grave violations of international law, including acts for which the International Criminal Court (ICC) has issued arrest warrants for Israeli Prime Minister Benjamin Netanyahu and former Defense Minister Yoav Gallant.

From Code to Kill Lists

As Israel intensified its assault on Gaza, its demand for AI and cloud-based technologies, supplied by US tech giants, grew rapidly, embedding corporate infrastructure into the machinery of war. In March 2024, Google deepened its ties with the Israeli Ministry of Defense (IMOD) by signing a new contract to build a specialized "landing zone" into its cloud infrastructure, enabling multiple military units access to its automation technologies. Amazon Web Services (AWS), Google's partner in Project Nimbus, was reported to have supplied Israel's Military Intelligence Directorate with a

dedicated server farm capable of endless storage for surveillance data collected on almost everyone in Gaza.

Recent reporting has further documented the rapid expansion of Israel's AI-driven military capabilities, underscoring how growing partnerships with technology companies have accelerated the deployment of advanced systems in its war on Gaza. According to leaked documents, Microsoft hosted elements of the Israeli military's mass surveillance program on its cloud servers, storing recordings of millions of intercepted phone calls from Palestinians in Gaza and the West Bank. The Israeli occupation forces reportedly used these files to identify bombing targets, blackmail individuals, place people in detention, and also to justify killings after the fact. The Israeli military's reliance on Microsoft Azure surged accordingly: in the first six months of the war, its average monthly use rose by 60%, while use of Azure's machine-learning tools increased 64-fold compared to prewar levels. By March 2024, the use of Microsoft and OpenAI technological tools by Israeli forces was nearly 200 times higher than it had been in the week preceding October 7, 2023. In addition, the amount of data stored on Microsoft's servers had doubled to more than 13 petabytes.

The results of Microsoft's own internal review, announced in September 2025, ultimately confirmed that a unit of the Israeli defense ministry had indeed used some of its services for prohibited surveillance purposes. Consequently, the company suspended certain cloud and AI services, admitting that its technology was complicit in practices that contravened its terms of service. Yet Microsoft's suspension of services to the Israeli military was minimal: many contracts and functions with the Israeli military and other government bodies responsible for gross human rights abuses and atrocity crimes remain intact. While the review itself is still ongoing, this narrow admission lays bare the company's complicity in Israel's military machinery.

Moreover, big tech's involvement in Israel's war appears to extend beyond standard service provision. Microsoft engineers have reportedly provided both remote and on-site technical assistance to Israeli forces, including Unit 8200 (cyber operations and surveillance) and Unit 9900 (geospatial intelligence and targeting). In fact, the Israeli defense ministry procured approximately 19,000 hours of Microsoft engineering and consultancy services, valued at around $10 million. Amazon has likewise been implicated, reportedly providing not only cloud infrastructure but also direct assistance in verifying targets for airstrikes. Google's role raises additional concerns: according

to internal documents, the company created a classified team composed of Israeli nationals with security clearances, tasked explicitly with receiving sensitive information from the Israeli government that could not be shared with the broader company. This team is set to deliver "specialized training with government security agencies" and to participate in "joint drills and scenarios tailored to specific threats." No comparable arrangement seems to exist between Google and any other state, underscoring the exceptional depth of its collaboration with the Israeli regime.

Profit is not the sole driver of big tech's deepening entanglement with Israel's military; political affinity plays a role as well. Palantir Technologies, a US-based data analytics and surveillance company known for its close ties to intelligence and defense agencies, has openly expressed support for Israel throughout the Gaza genocide. Palantir has partnered with AWS to deliver tools designed to help clients, such as the Israeli military, "win in the warfighting context." The company signed a strategic partnership with the Israeli defense ministry to provide technologies directly supporting the genocidal campaign. Microsoft, too, has longstanding ties with Israel's military and security apparatus—ties so close that Netanyahu once described the relationship as "a marriage made in heaven but recognized here on earth."

By providing direct support to Israeli military operations, tech companies are not merely supplying infrastructure; they are actively facilitating and aiding the surveillance, targeting, and execution of actions that violate international law. In a grim evolution, the deployment of commercial AI in Gaza marks a chilling frontier: systems once designed to optimize logistics and decision-making at scale are now generating kill lists, erasing families, and leveling entire neighborhoods. Technology developed and maintained by big tech now underpins warfare, ethnic cleansing, and genocide in Palestine, serving as a prototype for the future of automated warfare.

The Future of Warfare

The Israeli regime has formalized its push toward automated warfare by creating a dedicated AI research division within the IMOD, tasked with advancing military capabilities for a future in which "battlefields will see integrated teams of soldiers and autonomous systems working in concert." This initiative marks a significant shift toward the normalization of AI-driven combat. Western governments, including France, Germany, and the US, are pursuing similar trajectories, racing to

integrate artificial intelligence into their weapons systems and armed forces. Together, these developments position Israel not only as an early adopter but as a model for the coming era of algorithmic warfare.

In parallel, major tech companies are abandoning their self-imposed ethical boundaries in pursuit of military contracts. Earlier this year, both Google and OpenAI quietly abandoned their voluntary commitments not to develop AI for military use, signaling a broader realignment with the security and defense sectors. Within weeks of amending its AI principles, Google signed a formal partnership with Lockheed Martin, the world's largest arms manufacturer and a major supplier of weapons to the Israeli military. In November 2024, Meta announced that it would make its large language models, called Llama, available to US government agencies and contractors working on national security. Lockheed Martin has since integrated Llama into its operations.

Joining the AI-for-warfare race, Meta has also partnered with Anduril, a defense technology startup, to develop virtual and augmented reality devices for the US Army. Despite its nonprofit status, OpenAI collaborated with Anduril to deploy its technology on the battlefield. In addition, Palantir and Anthropic—an AI research and development company backed by Google—announced a partnership with AWS to "provide US intelligence and defense agencies access" to its AI systems.

A telling indicator of the deepening convergence between big tech and ministries of war is the US Army's decision to grant senior executives from Palantir, Meta, OpenAI, and Thinking Machines Labs the rank of lieutenant colonel and to embed them as advisors within the armed forces. Framed as an effort to "guide rapid and scalable tech solutions to complex problems," the initiative seeks to make the US military "leaner, smarter, and more lethal." The symbolism is hard to miss: Silicon Valley leaders are no longer merely building tools for the battlefield; they are being formally integrated into its command structure.

AI Militarization in a Regulatory Vacuum

AI militarization is rapidly unfolding in the absence of effective regulatory frameworks. While states continue to deliberate norms for autonomous weapons at the UN, no binding international treaty specifically governs their development or deployment. Even less regulated are dual-use technologies, such as LLMs and cloud infrastructure, which

are now being embedded in military operations. Recent national and global conversations and regulatory proposals regarding AI governance, which often focus on upholding privacy and human rights, largely sidestep the devastating impact of AI systems in conflict zones. The most illustrative example of this disconnect is Israel's signing of the Council of Europe's AI treaty, which addresses human rights, democracy, and the rule of law, at a time when credible reports were emerging about its use of AI-driven targeting in Gaza. While the treaty contains numerous caveats that limit its effectiveness, Israel's signature amid an ongoing campaign of genocide underscores the profound disconnect between the legal norms being crafted and the battlefield deployment of the technologies they seek to regulate.

Meanwhile, voluntary guidelines or soft-law mechanisms are routinely discarded. The UN Guiding Principles on Business and Human Rights (UNGPs), which outline both state obligations and corporate responsibilities to identify and mitigate human rights risks, are frequently ignored by tech companies. While these principles clearly state that companies operating in conflict zones must treat the risk of contributing to gross human rights abuses and violations of international humanitarian law as a legal compliance issue, tech companies continue to comply selectively. Microsoft's belated admission that the Israeli regime used its cloud infrastructure for mass surveillance in Gaza is a case in point. In May 2025, Microsoft denied enabling the Israeli regime to inflict harm on Palestinians through mass surveillance, only to reverse course months later with a narrow admission of misuse of its technology. As mentioned, this admission exposes the extent to which companies fail to fulfil their responsibility under the UNGPs to identify and mitigate such harm.

Source: https://al-shabaka.org/briefs/ai-for-war-big-tech-empowering-israels-crimes-and-occupation/

Image: Source [Edited]

Original Article: https://www.thelibertybeacon.com/silicon-valleys-ai-infrastructure-behind-gaza-genocide/

COMMENTS (0)

Subscribe to Truth11.com

Receive Articles By Email • Support Independent Media

Subscribe now

Support Truth11.com | • Make A Donation

• Become A Monthly Subscriber

© Truth11.com 2025